Postfix als sicheres SMTP-Gateway

Ralf Hildebrandt
innominate AG
hildeb@codeblau.de

30. März 2002

Sicherheit

Sicherheit ist ein dynamischer Prozeß

- Installation ist nicht genug ("shoot-yourself-in-the-foot")
- massive Fluktuationen

Open Source

Sicherheitstechnologien müssen ausgereift und sicher sein.

Open Source Software garantiert ein Höchstmäß an Sicherheit durch die offene und herstellerunabhängige Entwicklung.

Zusätzlich ist sie extrem stabil und leistungsfähig.

Deshalb wird Open Source auch von der NSA und dem deutschen BSI empfohlen.

innominate Security Approach

- Angebot von IT-Sicherheitslösungen
  - Angebot von IT Sicherheitslösungen
  - Basis Open Source Software
  - Dienstleistungen
- Modulares Angebot
  - Analyse
  - Konzeption
  - Implementation
  - Support
  - Betrieb
  - Überwachung
  - Anpassung an Bestand
- Neukonzeption

Überblick

- Anforderungen an einen Firewall-MTA
- Produktvergleich
- Warum Postfix?
- “Security by design”
- Modularität von Postfix
- Design & Features
- Ein Firewall-Setup
- Benutzer von Postfix
- Fragen und Diskussion

Anforderungen an einen MTA

Das System. . .

- Sicherheit und Zuverlässigkeit
  - ist dem Internet direkt ausgesetzt
  - ist ein point-of-failure für die Unternehmens-Email
  - ist nicht ständig warten zu müssen
- Geschwindigkeit
  - muß den gesamten Traffic bewältigen können
- Features
  - muß (bei Bedarf) die Features des dahinter befindlichen MTA ergänzen können, z.B. durch:
    - Virenscanner
    - Spamschutz
    - Verbergen der internen Netzstruktur
    - sonstiges

Produktvergleich

20 gute Gründe[1] kein Sendmail zu verwenden

Advisory	Programm	Effekt
CA-88:01	Sendmail 5.58	run any command (debug)
CA-90:01	SUN Sendmail	root shell (remote)
CA-91:01a	SUN /bin/mail	root shell (local)
CA-91:13	ULTRIX /bin/mail	root shell (local)
CA-93:15	SUN Sendmail	write any file (remote)
CA-93:16	Sendmail 8.6.3	run any command (from)
CA-94:12	Sendmail 8.6.7	root shell (-d bignumber) read any file (-oE filename)
CA-95:02	/bin/mail	write any file (race)
CA-95:05	Sendmail 8.6.9	any command/file (ident)
CA-95:08	Sendmail V5	any command/file
CA-95:11	SUN Sendmail	root shell (-oR host -f cmd)
CA-95:13	Sendmail 8.7.0	root shell (syslog)
CA-96.04	Sendmail 8.7.3	root shell (dns newline)
CA-96.20	Sendmail 8.7.5	root shell (fullname buffer) default uid/gid (getpwuid)
CA-96.24	Sendmail 8.8.2	root shell (argv[0])
CA-96.25	Sendmail 8.8.3	group id (:include:, .forward)
CA-97.05	Sendmail 8.8.4	root shell (MIME buffer)
	Sendmail 8.8.8	group-/world writable forward, :include:, class, ErrorHeader, or HelpFile
	Sendmail 8.9.1	sleep(5) Denial of Service attack
	Sendmail 8.9.2	headers Denial of Service attack

[1] siehe auch http://cr.yp.to/maildisasters/sendmail.html

Produktvergleich

Name	Sicherheit	Zuverlässigkeit	Geschwindigkeit	Features
sendmail	−/o	+	−/o	++
qmail	+/++	+/++	+	−
postfix	++	++	++	+
exim	o	+	+	++
smap	?	mir graut	?	?

Fazit: Postfix (oder qmail[2])

[2] it's a question of style

Secure-by-Design

- "principle of least privilege"
- `chroot`
- spezielle I/O Routinen mit dynamischer Allozierung von Puffern
- Resourcenbeschränkung
- Modularität
- kein Modul traut den Daten, die es von einem anderen erhält
- keine direkte Verbindung vom Netz zur privilegierten lokalen Zustellung
- Der Autor:
  - tcp_wrappers
  - SATAN
  - tct (*The Coroner's Toolkit)*

Modularität

Design & Features

- Einfachheit
  - Installation dauert ca. 5 Minuten
  - Legacy Systeme werden unterstützt (OSF/1)
  - keine kryptische `sendmail.cf`
  - lesbare Konfigurationsdatei (auch ohne `m4`)
- Robustheit und Stabilität
  - Postfix verliert nicht die Kontrolle
  - Mail geht nicht verloren
- Geschwindigkeit
  - Platten I/O allein beschränkt die Geschwindigkeit.
  - minimierte Anzahl von Schreiboperationen:
    Pro Nachricht wird höchstens 1 Datei auf Platte geschrieben (qmail: 3)

Design & Features II

- Spam/UCE Kontrolle
  - DNS-basierte "schwarze Listen" (RBL, RSS, ORBS, DUL)
  - syntaktische Kontrollen gem. der einschlägigen RFCs
  - Abweisung nach Client, Sender, Recipient, Header und/oder Body
  - Abweisung von Clients, Senders und/oder Recipients, die keinen DNS-Eintrag haben
- `Sendmail`-Kompatibilität
  - `sendmail`
  - `newaliases`
  - `mailq`
  - ... man muss nicht einmal das Startscript aendern!
- schnelle Updates
  - Ein Update ist mit Downtime von unter 5s möglich
- SQL- und LDAP-Anbindung
  - für alle Maps

Ein simples Firewall-Setup

Der Inhalt von /etc/postfix/main.cf:

```
myorigin = $mydomain
mydestination = $mydomain
transport_maps = hash:/etc/postfix/transport

mynetworks =
   ip.von.inside-gateway.domain/32,
   127.0.0.1/8
```

Der Inhalt von /etc/postfix/transport:

```
domain.com   inside-gateway.domain.com
```

Alle anderen Parameter sind auf sinnvolle Standardwerte gesetzt und sollten außer bei bizarren IT-Strukturen keiner Änderung benötigen.

Konfiguration – fortgesetzt

/etc/postfix/master.cf:

```
#==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (50)
#==========================================================================
smtp      inet  n       -       -       -       -       smtpd
pickup    fifo  n       n       -       60      1       pickup
cleanup   unix  -       -       -       -       0       cleanup
qmgr      fifo  n       -       -       300     1       qmgr
#qmgr     fifo  n       -       -       300     1       nqmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
flush     unix  -       -       -       1000?   0       flush
smtp      unix  -       -       -       -       -       smtp
showq     unix  n       -       -       -       -       showq
error     unix  n       -       -       -       -       error
#local     unix  -       n       n       -       -       local
```

Benutzer von Postfix

- bugtraq.com
  "Bugtraq (securityfocus) uses Postfix. In private conversation (USENIX Security last year) Aleph told me that Postfix sped up their deliveries over qmail by a wide margin."
- hp.com
  aber nicht für Ihr eigenes HP-UX. . .
- pobox.com
- listman.redhat.com
- innominate.com
- SuSE
- berliner-volksbank.de
- charite.de
- seb.de
- spin.it
- freebsd.org
- compaq.com
- python.org
- gnome.org

- amazon.com
- bundestag.de

Links

- Postfix Website (`http://www.postfix.org`):
  - FAQ
  - Quellcode
  - Mailinglisten-Archive
  - Patches
- Postfix von Richard Blum
- `Logfile Summary` (`http://jimsun.linxnet.com/postfix_contrib.html`)
- 07000-POSTFIX